Stubblebine 109755con-1

IN THE CLAIMS:

52. (Original) A method for system security in distributed systems, comprising the steps of:

a) deriving freshness constraints from initial policy assumptions and an authentic statement;

b) imposing freshness constraints by employing recent-secure authenticating principals to effect revocation; and

c) verifying that a relation f $\left|t_{now} - t_{time\ stamp}\right| \leq \delta$ is satisfied for verification of a secure channel, where $t_{time\ stamp}$ being a time of a time stamp pertaining to a validity assertion of a particular assertion, $\delta$ being a minimum necessary freshness constraint pertaining to the particular assertion and $t_{now}$ being the time of verification;

53. (Currently Amended) A system for enforcing revocation in distributed systems, comprising:

a) means for ~~asserting~~ creating a time-stamped validity assertion message pertaining to the validity of an initial assertion;

b) means for asserting a freshness constraint[[s]] indicating a length of time, and relating to said initial assertion ~~the initial assertions that the freshness constraints relate to~~; and

c) means for verifying that a relation $\left|t_{now} - t_{time\ stamp}\right| \leq \delta$ is satisfied ~~for each particular assertion necessary for verification of a secure channel~~, where $t_{time\ stamp}$ is a ~~time of~~ a time stamp contained in said message ~~pertaining to the validity assertion of a particular assertion~~, $\delta$ ~~being~~ is a selected constant that represents a minimum necessary freshness constraint pertaining to said initial assertion ~~the particular~~ assertion, and $t_{now}$ is ~~being the~~ time of verification.

54. (Currently Amended) A system for protecting an authority of a distinguished principal and enforcing revocation when the authority is compromised, comprising:

Stubblebine 109755con-1

a) a first means-for issuing an authoritative assertion by a distinguished principal;

b) a second means for asserting freshness constraints on the assertion;

c) a third means for asserting a time stamped validity assertion to the assertion indicating the validity of the assertion at the time of the time stamp; and

d) means for verifying that a relation $|t_{now} - t_{time\ stamp}| \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being the time of a time stamp pertaining to the validity assertion of the particular assertion, $\delta$ being the minimum necessary freshness constraint pertaining to the particular assertion, and $t_{now}$ being the time of verification.

55. (Original) A system for issuing certificates in a system for enforcing revocation in distributed systems, comprising:

a) means for issuing certificates for principals within an organization by the organization;

b) means for asserting, by the organization, a principal authorized as an authority for issuing time stamped certificates;

c) means for delegating authority for issuing time stamped certificates;

d) means for asserting freshness constraints on assertions; and

e) means for verifying that a relation $|t_{now} - t_{time\ stamp}| \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, $\delta$ being a minimum necessary freshness constraint pertaining to the particular assertion and $t_{now}$ being the time of verification.

56. (Original) A system for system security in a distributed system network, comprising:

Stubblebine 109755con-1

a) means for preparing a statement of an assigned revocation authority in a distributed system network in response to a policy, said revocation authority statement being associated with an initial statement;

b) means for preparing a statement of a freshness constraint period in the distributed system network in response to said policy, said freshness statement being associated with said revocation authority statement;

c) means for preparing a validity statement at said assigned revocation authority in the distributed system network in response to said policy, said validity statement including a verification status at some temporal reference;

d) means for providing said revocation authority statement, said freshness statement, and said validity statement to a verification authority in the distributed system network; and

e) means for selectively verifying said initial statement at said verification authority in response to said initial statement, said revocation authority statement, said freshness statement, and said validity statement.